

# The Sarbanes-Oxley Act of 2002

Strategies for Meeting New Internal Control  
Reporting Challenges: A White Paper



This white paper provides companies affected by the Sarbanes-Oxley Act of 2002 with general information and considerations regarding internal control reporting requirements. The information and considerations presented do not constitute legal advice. Companies are encouraged to consult with legal counsel concerning their responsibilities under and compliance with the statute and related Securities and Exchange Commission (SEC) rules and regulations.

# Contents

<b>I. Preface</b>	2
Why Sarbanes-Oxley Was Enacted	2
The Legislation of Accountability	2
<i>Sarbanes-Oxley's Impact on the Corporate Reporting Supply Chain</i>	3
How This White Paper Can Help	5
<b>II. Sarbanes-Oxley Reporting Challenges</b>	6
CEO and CFO Certification: The First Challenge	6
<i>Disclosure Controls and Procedures</i>	7
<i>Internal Controls and Procedures for Financial Reporting</i>	8
Internal Control Report and External Auditor Attestation: The Second Challenge	9
<b>III. Strategies and Actions for Achieving Reporting Compliance</b>	10
Starting with a Framework for Internal Control	10
<i>COSO Internal Control Framework</i>	10
<i>Internal Controls and Procedures for Financial Reporting</i>	13
<i>Disclosure Controls and Procedures</i>	15
<i>The Risks of an Informal Control Process</i>	16
Operationalising the Control Process	17
<i>The Benefit of Using an Internal Controls Maturity Framework</i>	17
<i>Developing an Action Plan and Beyond</i>	19
Aligning Reporting Obligations with Strategic Management	22
<i>Strategic Management Needs</i>	22
<i>Linking Enterprise-Wide Risk Management with Sarbanes-Oxley</i>	23
<b>IV. Conclusion: A New Beginning</b>	24
<b>Appendix A: Summary of the Sarbanes-Oxley Act of 2002</b>	25
<b>Appendix B: Effective Dates of Principal Provisions in Sarbanes-Oxley Titles III and IV</b>	27

# I. Preface

## Why Sarbanes-Oxley Was Enacted

The Sarbanes-Oxley Act of 2002<sup>1</sup> (Sarbanes-Oxley) was enacted on July 30, 2002, largely in response to a number of major corporate and accounting scandals involving some of the most prominent companies in the United States. These scandals have resulted in a great loss of public trust in corporate accounting and reporting practices.

CEOs and CFOs of public companies must firmly grasp the degree and significance of distrust that now exists. For example, according to some surveys:

- 77% of the public believe that CEO greed and corruption have caused the U.S. financial meltdown – *CNN / USA Today Poll, July 2002*.
- 71% of investors say accounting fraud is rampant – *Survey of Main Street Investors, July 2002*.
- 82% of investors believe that tough new laws are needed – *Harris Poll, July 2002*.
- 54% of portfolio managers say not just a few bad apples among companies – *F.D. Morgan Walke Poll, August 2002*.
- 81% of fund managers and analysts think executives place their own interests ahead of shareholders – *Broadgate Consultants, March 2002*.
- 71% of fund managers say executive pay is too high, 0% say it is too low or just right – *Pearl Meyer, June 2002*.
- 70% of the corporate frauds studied between 1987 and 1999 involved the CEO – *The Wall Street Journal, "Auditors' Methods Make It Hard to Catch Fraud by Executives," July 8, 2002*.

With public sentiments such as these as a backdrop, Sarbanes-Oxley was enacted in a major effort to prevent accounting scandals and other reporting problems from recurring, and to rebuild public trust in corporate business practices and reporting.

## The Legislation of Accountability

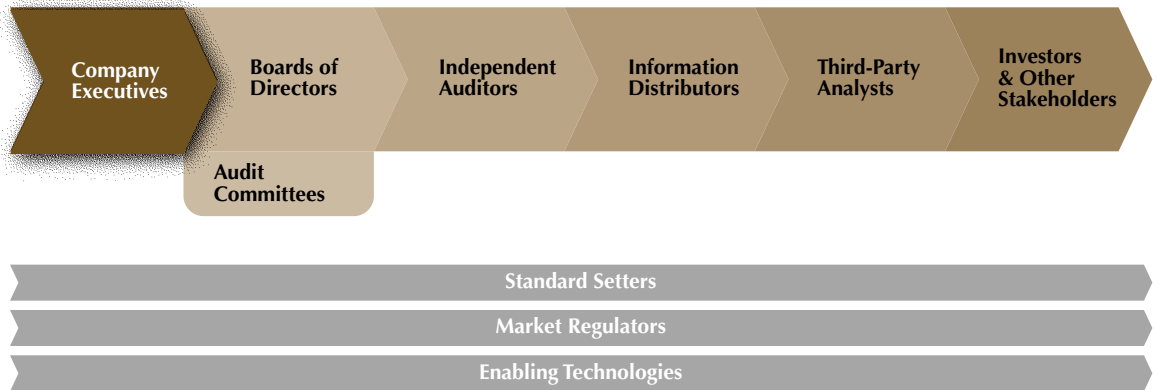
Sarbanes-Oxley establishes new or enhanced standards for corporate accountability and penalties for corporate wrongdoing. The legislation contains 11 titles, ranging from additional responsibilities for audit committees to tougher criminal penalties for white-collar crimes such as securities fraud. Many of the legislation's provisions direct the SEC to issue implementing guidance.

A brief summary of each of Sarbanes-Oxley's titles is provided in Appendix A.

Without question, these new requirements place increased demands on some companies' executives and internal resources as well as others involved in corporate reporting. To restore the credibility of corporate accounting and reporting, Sarbanes-Oxley defines a higher level of responsibility, accountability, and financial reporting transparency – changes that ultimately are intended to return to investors the confidence they need to once again become active in the nation's financial markets.

# Sarbanes-Oxley's Impact on the Corporate Reporting Supply Chain

## The Corporate Reporting Supply Chain\*



PricewaterhouseCoopers recently published *Building Public Trust – The Future of Corporate Reporting*, in which our CEO, Sam DiPiazza, describes the “corporate reporting supply chain,” how it works, and how it can be improved to regain public trust in corporate reporting.<sup>2</sup> The key players in this supply chain are:

1. Company executives who prepare or approve the information distributed to investors and other stakeholders.
2. Boards of directors who represent these stakeholders’ interests and are responsible for governance and oversight of management activities on their behalf.
3. Independent auditors who provide assurance on financial statements and other information distributed in the capital markets.
4. Information distributors that consolidate reported information and provide it to others for use.
5. Third-party analysts who use company-provided information and their own analysis to make investor recommendations.
6. Investors and other stakeholders who are the ultimate consumers of corporate reporting information.

A primary objective of *Building Public Trust* was to identify and encourage certain behaviours by all the key players in the corporate reporting supply chain that are intended to result in more reliable, timely, and useful information to assist stakeholders in their decision-making process.

\* *Standard Setters* refers to organisations that set accounting and auditing standards, as well as others in similar roles. *Market Regulators* include governmental agencies and other bodies that set and enforce rules relating to corporate reporting. *Enabling Technologies* contribute to the widespread distribution and use of reported information.



Sarbanes-Oxley requires that company executives, boards of directors, and independent auditors take specific actions to achieve a similar goal for corporate reporting. A central theme of Sarbanes-Oxley is how these key players in the supply chain must work together, with critical cross-checks, to achieve that goal. To carry out this theme, Sarbanes-Oxley reinforces and expands on the responsibilities of these players in the corporate reporting supply chain:

## 1. Company Executives

Sarbanes-Oxley reaffirms that the CEO and CFO carry a primary responsibility for a company's reports filed with the SEC and institutes a requirement for them to report on the completeness and accuracy of the information contained in the reports as well as the effectiveness of underlying controls.

Sarbanes-Oxley establishes a standard that is broader than GAAP, indicating that the CEO and CFO must provide financial statements and other financial information that is transparent in the way it fairly presents the company's financial condition, results of operations, and cash flows.

## 2. Board of Directors and Audit Committees

Sarbanes-Oxley establishes new responsibilities for the audit committee in its capacity as a committee of a board of directors, including the appointment and compensation of the external auditor and oversight of the auditor's work for the purpose of preparing or issuing an audit report or related work. It also establishes that the external auditor is to report directly to the audit committee.

The legislation requires the audit committee to pre-approve all services, regardless of their nature, that are provided by the external auditor. Moreover, each audit committee must comprise independent directors, as defined, and the company must disclose, among other things, whether at least one member of the committee meets the specified criteria of an "audit committee financial expert" and, if not, the reasons why.

## 3. External Auditor

An external auditor reports on the fairness of the presentation of a company's financial statements in accordance with generally accepted accounting principles. Sarbanes-Oxley reaffirms the necessity for the auditor to be independent of management, in fact and appearance, and expands the auditor's reporting responsibility to an attestation of the newly required management assertions on internal controls and procedures for financial reporting.



## How This White Paper Can Help

This white paper focuses primarily on the *reporting obligations of company executives* as to the completeness and accuracy of information contained in company reports and the effectiveness of underlying internal controls. These new reporting obligations are covered by Titles III and IV of Sarbanes-Oxley and related SEC rules.

The purpose of this paper is twofold:

1. To help company executives, boards of directors, and audit committees of public companies<sup>3</sup> better understand the implications of these reporting obligations; and
2. To introduce strategies and actions developed by PricewaterhouseCoopers to help company management develop tailored plans and processes to manage their reporting obligations.

This paper is also intended to help other interested parties better understand the implications of the reporting obligations imposed by Sarbanes-Oxley.

While this paper focuses on the first player in the corporate reporting supply chain – company executives – our intention is to continue to pursue actions that will strengthen the entire chain and provide additional guidance in the future.

Beyond the guidance included herein, the following key elements, as discussed in *Building Public Trust*, are paramount for all players in the corporate reporting supply chain:<sup>4</sup>

- **Spirit of Transparency.** Companies have an obligation to provide willingly to shareholders and other stakeholders the information needed to make decisions. This information should be transparent in the way it presents a company's financial condition, results of operations, cash flows, and other aspects of its business.
- **Culture of Accountability.** Transparent information must be accompanied by a firm commitment to accountability among all players in the corporate reporting supply chain and those who define how it should work. Each player must take responsibility, in collaboration with all others, for carrying out its role in this chain.
- **People of Integrity.** Transparency and accountability depend on people of integrity trying to “do the right thing,” not just what is expedient or even permissible. Without personal integrity as the foundation for reported information, there can be no public trust.

## II. Sarbanes-Oxley Reporting Challenges

Sarbanes-Oxley has established a new requirement that CEOs and CFOs explicitly evaluate and report to the public on the effectiveness of specified internal controls over corporate reporting. This reporting requirement is contained primarily in Title III of the legislation, "Corporate Responsibility," and in Title IV, "Enhanced Financial Disclosures." This paper examines these provisions and their implications.

Appendix B provides a recap of the effective dates of the principal provisions directly affecting public companies in Titles III and IV of Sarbanes-Oxley and related SEC rules.


### CEO and CFO Certification: The First Challenge

As directed by Title III, §302 of Sarbanes-Oxley, the SEC has issued a certification rule, "Final Rule: Certification of Disclosure in Companies' Quarterly and Annual Reports," effective August 29, 2002.<sup>5</sup> This rule requires that, as part of each quarterly and annual report filed by a public company under the Exchange Act of 1934, the CEO and CFO must provide certifications containing several representations as summarised below:

1. They have reviewed the report.
2. Based on their knowledge, the report contains no untrue statement of a material fact and does not omit any material fact that would cause any statements to be misleading.
3. Based on their knowledge, the financial statements and other financial information in the report fairly present, in all material respects, the company's financial position, results of operations, and cash flows.
4. They are responsible for and have designed, established, and maintained disclosure controls and procedures, and the report presents conclusions about the effectiveness of disclosure controls and procedures based on their evaluation within 90 days prior to the report's filing date (see "Disclosure Controls and Procedures" on page 7).
5. They have disclosed to the audit committee and external auditor (a) any significant deficiencies and material weaknesses in internal controls for financial reporting and (b) any fraud (material or not) involving anyone having a significant role in those internal controls.
6. They have disclosed in the report whether, after their most recent evaluation, significant changes occurred that affected internal controls for financial reporting, and whether any corrective actions were taken with regard to significant deficiencies and material weaknesses.

Representations 4, 5, and 6 are required as part of certifications with respect to reports covering periods ending after August 29, 2002.





The SEC certification rule specifies the form and exact wording to be used for certifications in specific types of reports, and directs that no deviations be allowed. Counsel may need to be consulted if there is any doubt about whether standard wording appropriately covers a company's unusual circumstances.

The SEC has dictated that CEOs and CFOs must certify the following reports:

- Annual reports on Forms 10-K, 10-KSB, 20-F, and 40-F<sup>6</sup>
- Quarterly reports on Forms 10-Q and 10-QSB
- Amendments to, and transition reports on, any of the foregoing reports

## Disclosure Controls and Procedures

The SEC certification rule uses a new term – “disclosure controls and procedures” – defined as:

“Controls and other procedures of an issuer that are designed to ensure that information required to be disclosed by the issuer in the reports filed or submitted under the Exchange Act is recorded, processed, summarized, and reported within the time periods specified in the Commission’s rules and forms. ‘Disclosure controls and procedures’ include, without limitation, controls and procedures designed to ensure that information required to be disclosed by an issuer in its Exchange Act reports is accumulated and communicated to the issuer’s management ... as appropriate to allow timely decisions regarding required disclosure.”

According to this rule, disclosure controls and procedures:

“... are intended to cover a broader range of information than is covered by an issuer’s internal controls related to financial reporting.... They are intended to ensure that an issuer maintains commensurate procedures for gathering, analyzing and disclosing all information that is required to be disclosed in its Exchange Act reports.”

The rule collectively imposes an explicit *reporting obligation* with respect to disclosure controls and procedures, requiring CEOs and CFOs to certify in specified annual or quarterly reports filed with the SEC that they are responsible for establishing and maintaining disclosure controls and procedures for the company and that they have:

- Designed such disclosure controls and procedures to ensure that material information relating to the company is made known to them.
- Evaluated their effectiveness within 90 days prior to the report’s filing date.<sup>7</sup>
- Presented conclusions about their effectiveness in the report.

The SEC has recommended that, to assist CEOs and CFOs in executing that responsibility, each company have a “disclosure committee” with responsibility for considering the materiality of information and determining required disclosures to the public on a timely basis.



With regard to performing evaluations quarterly, the SEC has stated that:

“While the new rules do not provide detailed guidelines for such an evaluation, the evaluation must, at a minimum, address the matters specified by the [SEC] rules. We expect that this evaluation would be carried out in a manner that would form the basis for the certification statements....”

The implementation issues associated with this new reporting obligation are addressed in section III of this paper.

## Internal Controls and Procedures for Financial Reporting

The SEC certification rule states that “financial statements and other financial information” as used in the certification refers to:


“... financial statements (including footnote disclosure), selected financial data, management’s discussion and analysis of financial condition and results of operation and other financial information in a report.”

The new rule also interprets “fair presentation of financial statements” to mean a standard that is broader than merely complying with generally accepted accounting principles, as follows:

“The certification statement regarding fair presentation of financial statements and other financial information is not limited ... by reference to generally accepted accounting principles. We believe that Congress intended this statement to provide assurances that the financial information disclosed in a report, viewed in its entirety, meets a standard of *overall material accuracy and completeness* [emphasis added] that is broader than financial reporting requirements under generally accepted accounting principles. In our view, a ‘fair presentation’ of an issuer’s financial condition, results of operations and cash flows encompasses the selection of appropriate accounting policies, proper application of appropriate accounting policies, disclosure of financial information that is informative and reasonably reflects the underlying transactions and events and the inclusion of any additional disclosure necessary to provide investors with a materially accurate and complete picture of an issuer’s financial condition, results of operations, and cash flows.”

Translated, we believe this statement is aligned with the spirit of transparency required of all members of the corporate reporting supply chain.





The new rule requires quarterly reports to disclose whether a company's internal controls and procedures for financial reporting have been affected by any significant changes "subsequent to the date of their evaluation" – but it does not specifically require a separate evaluation of those internal controls. A subsequent SEC proposal:<sup>8</sup>

- States that the SEC believes "... a significant portion of internal controls and procedures for financial reporting are included in disclosure controls and procedures."
- If adopted, would amend the SEC's certification rule so as to explicitly require that a company's management evaluate on a quarterly basis the effectiveness of internal controls and procedures for financial reporting, as well as disclosure controls and procedures.

## Internal Control Report and External Auditor Attestation: The Second Challenge

As directed by Sarbanes-Oxley Title IV, §404, the SEC has proposed a rule<sup>9</sup> that, if adopted, would require each *annual* report issued by a company under the Exchange Act<sup>10</sup> to contain an internal control report stating:

- Management's responsibility for establishing and maintaining adequate internal controls and procedures for financial reporting.
- Management's conclusions about the effectiveness of internal controls and procedures for financial reporting as of year-end, based on management's evaluation.
- That the external auditor has attested to, and reported on, management's evaluation.

This proposed rule does not specify the exact content of management's internal control report, indicating only that "management should tailor the report to the company's circumstances." What is obvious, however, is that the company's internal controls and procedures for financial reporting and management's evaluation of them must be documented in a manner to permit review by others.

The proposed SEC rule also requires a company's external auditor to attest to management's assertions about internal controls and procedures for financial reporting. It does not establish standards for the contents of an attestation report, but requires that the attestation be performed in accordance with standards issued or adopted by the Public Company Accounting Oversight Board, once the new board becomes operational. Until those standards are adopted, existing and widely accepted standards for performing attestations can be found in AICPA attestation standards.<sup>11</sup>

The SEC has proposed making its implementation rules for §404 effective beginning with annual reports for fiscal years ending on or after September 15, 2003.

The obligation to issue this internal control report that must be attested to by the external auditor raises a number of implementation issues, several of which are addressed in Section III of this paper under the sub-heading "Internal Controls and Procedures for Financial Reporting."

### III. Strategies and Actions for Achieving Reporting Compliance

CEOs and CFOs carry a heavy burden of responsibility for their companies' internal controls. Provisions in Sarbanes-Oxley and recent SEC rulemaking make it clear that they are responsible for (1) establishing and maintaining disclosure controls and procedures, (2) designing disclosure controls and procedures to ensure that specified information is made known to them, and (3) undertaking regular evaluations of disclosure controls and procedures in connection with quarterly certifications and other reporting obligations. Sarbanes-Oxley also imposes a new requirement upon company management to assert to and report on the effectiveness of a company's internal controls and procedures for financial reporting on an annual basis. In addition, a recent SEC proposal would amend the existing quarterly CEO and CFO certification requirements to explicitly require a quarterly evaluation of those controls and procedures. Congress put noticeable teeth in these responsibilities by instituting tough civil and criminal penalties for knowingly certifying to the SEC a report that contains material misstatements or omissions.

Stated simply, companies have no choice as to whether to put effective controls in place and report on them as required by the SEC. The only real decision to be made is *how* to achieve compliance and a culture of accountability that supports it.

The remainder of this paper presents strategies and actions developed by PricewaterhouseCoopers to help CEOs, CFOs, and others involved in internal control develop plans and processes to manage their reporting obligations in a manner that will enhance public trust.

#### Starting with a Framework for Internal Control

Companies that are just beginning to formalise their risk management process and controls will find that a framework for internal control provides a helpful starting point and a solid foundation for building an effective internal control system.

This sub-section briefly describes the dynamics and components of a framework for internal control and how it can be used to establish and evaluate controls across an organisation. Next, several implementation issues are addressed that involve internal controls and procedures for financial reporting and disclosure controls and procedures, respectively. Finally, thoughts are provided about the risks of an informal control process, especially with respect to controls for which Sarbanes-Oxley requires evaluation and public reporting on their effectiveness.

#### COSO Internal Control Framework

"Internal control" means different things to different people, a problem that is compounded when the term is written into laws, rules, and regulations.

In the U.S., the most broadly accepted framework for internal control is provided by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).<sup>12</sup> In the spirit of transparency, we note that PricewaterhouseCoopers authored the COSO framework for the Committee of Sponsoring Organizations in 1992. Since that time, this framework has also been incorporated into U.S. auditing standards.<sup>13</sup> One of the benefits of COSO is that it establishes a common definition serving the needs of different people while providing a standard and criteria against which companies and organisations can assess or design their control systems.<sup>14</sup>

Many companies already have an internal control system based on the COSO framework. We recommend the COSO framework as an effective standard for establishing an internal control system that is tailored to a company's business environment. It can be especially helpful in the design, maintenance, and evaluation of internal controls and procedures for financial reporting and disclosure controls and procedures.

The COSO framework<sup>15</sup> and U.S. auditing standards<sup>16</sup> define "internal control" as a process – effected by an organisation's board of directors, management, and other personnel – that provides reasonable assurance regarding achievement of objectives in the following categories.

- **Effective and efficient operations.** Addresses a company's basic business objectives, including performance and profitability goals and the safeguarding of resources.
- **Reliable financial reporting.** Covers the preparation of reliable financial statements and other financial information.
- **Compliance with applicable laws and regulations.** Covers laws and regulations to which a company is subject, such as Sarbanes-Oxley and related rules, to avoid damage to a company's reputation or other negative consequences.

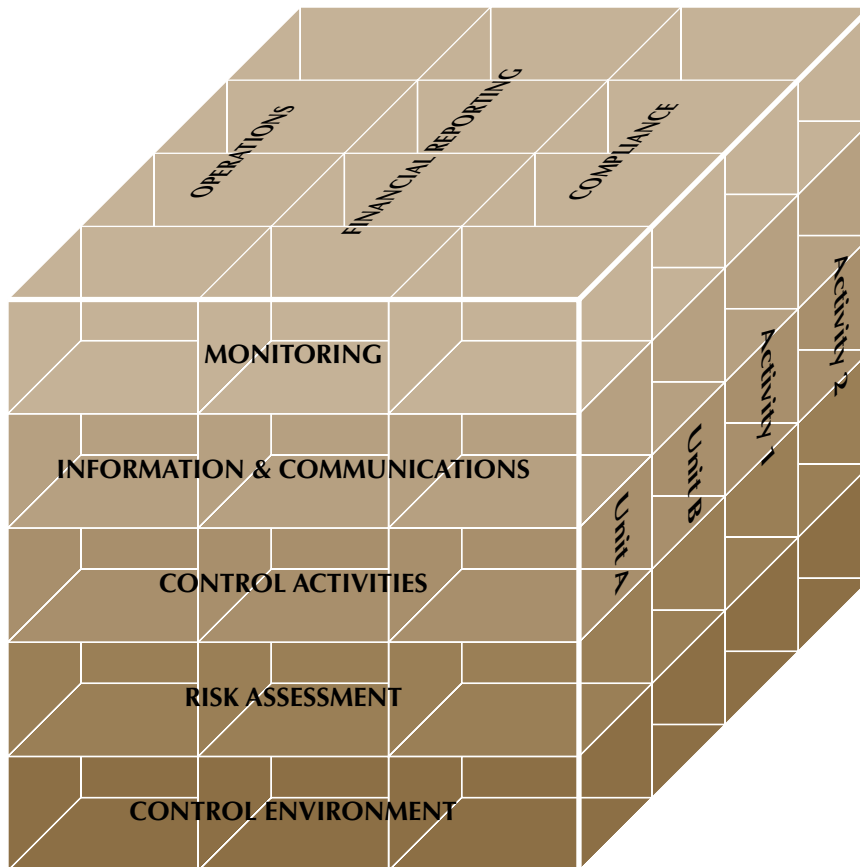
COSO identifies five components of internal control that need to be in place and integrated to achieve these objectives:<sup>17</sup>

- **Control environment.** Establishes the foundation for an internal control system by providing discipline and structure.
- **Risk assessment.** Involves the identification and analysis by management of relevant risks to achieving predetermined objectives, forming a basis for determining how those risks should be managed.
- **Control activities.** Refers to the policies and procedures to ensure that management objectives are achieved and risk mitigation strategies are carried out.
- **Information and communication.** Supports all other control components by communicating control responsibilities to employees and providing information in a form and time frame that allow people to carry out their duties.
- **Monitoring.** Covers the oversight of internal controls by management or other parties outside the process; or the application of independent methodologies, such as customised procedures or standard checklists, by employees within a process.



COSO uses the matrix shown below to illustrate the direct relationship between objectives and control components. The third dimension of the matrix shows the units or activities of an entity related to internal control.<sup>18</sup>


### Relationship Between Objectives and Components



With regard to financial reporting and compliance objectives, COSO states that:

"An internal control system can be expected to provide reasonable assurance of achieving objectives relating to the reliability of financial reporting and compliance with laws and regulations. Achievement of those objectives, which are based largely on standards imposed by external parties, depends on how activities within the entity's control are performed."<sup>19</sup>

While the internal control components are intended for use in companies of all sizes, many small and midsize companies have chosen to implement them less formally than larger companies, which usually take a more structured approach to internal control. Because Sarbanes-Oxley requires an external auditor's attestation of management's assertions concerning internal controls and procedures for financial reporting, some companies will need to increase the degree of formality for those controls to enable their review, as discussed below.



## Internal Controls and Procedures for Financial Reporting

The requirement to report on the effectiveness of internal controls and procedures for financial reporting raises a number of implementation issues. Several of these issues are examined here to help companies prepare for this eventual required reporting.

### Objectives

At this writing, the SEC has only proposed rules pertaining to a company's public reporting concerning its internal controls and procedures for financial reporting. In a recently issued proposal, the SEC stated:

"We believe that the purpose of internal controls and procedures for financial reporting is to ensure that companies have processes designed to provide reasonable assurance that:

- the company's transactions are properly authorized;
- the company's assets are safeguarded against unauthorized or improper use; and
- the company's transactions are properly recorded and reported

to permit the preparation of the registrant's financial statements in conformity with generally accepted accounting principles."<sup>20</sup>

Eventually, the specific objectives for internal controls and procedures for financial reporting, as promulgated by the SEC, will require harmonisation with auditor reporting standards issued or adopted by the Public Company Accounting Oversight Board pursuant to §103 of Sarbanes-Oxley.

Sometimes it is difficult to determine what specific controls fall within the scope of financial reporting. Often, for example, controls to accomplish operations or compliance objectives can also help accomplish financial reporting objectives. Examples of these include:

- **Operations.** Physical controls over inventory, legal settlements, production statistics, and facility usage.
- **Compliance.** Controls over patent expirations, income tax assessments, and fines for non-compliance.

Although rules and standards for reporting on internal controls and procedures for financial reporting pursuant to §404 and §103 of Sarbanes-Oxley have not been established, companies still need to establish reasonable guidelines and boundaries as a basis for identifying, designing, and maintaining controls and procedures for financial reporting. The COSO framework, or one that is similar, can be helpful in providing a reference point.

## Evaluating Effectiveness for Financial Reporting Controls and Procedures

In stating a conclusion about the effectiveness of its internal controls and procedures for financial reporting, a company needs to have a clear understanding of what its controls are and what “effectiveness” means. This starts with documentation of the internal controls and procedures for financial reporting. The issue of effectiveness is addressed by COSO and AICPA standards.

According to COSO, determining whether a particular internal control system is “effective” is a subjective judgement resulting from an assessment of whether the five components are present and functioning effectively. Their effective functioning provides the reasonable assurance that one or more of the primary objectives is achieved. Thus, these components are also criteria for effective internal control.

Although all five criteria must be satisfied, each component does not need to function identically, or even at the same level, in different entities. Some trade-offs may exist between components. Because controls can serve various purposes, controls in one component can serve the purpose of controls that might normally be present in another component. Additionally, controls can differ in the degree to which they address a particular risk, so that complementary controls, each with limited effect, together can be satisfactory.

These standards also focus on whether or not an internal control system has any “material weakness.” AICPA standards, for example, define a “material weakness” as a condition:

“... in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements caused by error or fraud in amounts that would be material in relation to the financial statements may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions.”<sup>21</sup>

By this definition, an internal control system for financial reporting that, taken as a whole, has a material weakness, cannot be deemed to be effective. If a significant deficiency is identified, the materiality of a possible misstatement in the company’s financial statements must be considered when deciding whether the deficiency constitutes a material weakness. Making that decision also requires a review of other facts and circumstances that may reduce the risk of misstatement, sometimes referred to as *compensating controls*.

We believe that the intent of Sarbanes-Oxley in this area is to establish a reporting standard focusing on the effectiveness of the system of internal controls for financial reporting *taken as a whole*. We believe that a company’s disclosure committee or similar group, in coordination with legal counsel, should develop a process that also considers individual, significant deficiencies in those internal controls, that allows for an evaluation of whether the combined effect of individual, significant deficiencies results in a material weakness and that provides for disclosure of these conditions to the company’s audit committee and external auditor.





## External Auditor Attestation

A company should also consider the implications of Sarbanes-Oxley §404's requirement that the external auditor attest to management's annual evaluation of the effectiveness of internal controls and procedures for financial reporting.

Management and the external auditor should discuss the scope of this attestation engagement, the type of internal control documentation expected to be needed, and the nature of and other documentation considerations regarding management's review process – key factors that must be addressed to enable the external auditor to attest to management's assertions in accordance with established professional standards and in a cost-effective manner.

One condition for auditor attestation is an identifiable set of suitable criteria that management uses to assess effectiveness and that the auditor, in turn, uses to test that assessment. Current attestation standards define the following attributes of suitable criteria:<sup>22</sup>

- **Objectivity.** Criteria should be free from bias.
- **Measurability.** Criteria should permit reasonably consistent measurements, qualitative or quantitative, of subject matter.
- **Completeness.** Criteria should be sufficiently complete so that those relevant factors that would alter a conclusion about subject matter are not omitted.
- **Relevance.** Criteria should be relevant to the subject matter.

Criteria that have been established by groups of experts and through due process are considered suitable. The COSO framework meets this test. Companies can also define their own criteria, which the current SEC proposals do not prohibit; but, for purposes of the attestation, these criteria would need to be explained in management's assertion. Consistent with our experience with reporting on internal controls over financial reporting pursuant to implementing regulations of the Federal Deposit Insurance Corporation Improvement Act of 1991, we expect the vast majority of companies will use COSO as their stated criteria.

## Disclosure Controls and Procedures

Every company must determine for itself what disclosure controls and procedures will be needed and thus covered in its CEO and CFO certifications. Although many disclosure controls and procedures cover financial reporting, additional controls supporting non-financial disclosures also need to be identified. Many companies may find it helpful to take a broad view of their operations, compliance, and other areas to determine what activities or events will trigger the need for upstream internal communications and disclosures in specified reports filed with the SEC.

Some examples of activities or events that may impact the need for disclosures and supporting controls include:

- **Operations.** Backlogs, changes in key contracts, legal proceedings, supply chain interruption, and termination of a major supplier or customer.
- **Compliance.** Approval or failure of a clinical trial, and a regulatory decision on a proposed merger or permissible business activity.



## Evaluating Effectiveness of Disclosure Controls and Procedures

In the adopting release to the certification rule, the SEC stated that each company should develop an evaluation process “that is consistent with its business and internal management and supervisory practices.”<sup>23</sup> While the CEO’s and CFO’s conclusions about the effectiveness of disclosure controls and procedures are required to be disclosed in quarterly and annual reports, no specific criteria are set forth in the rule for reaching this conclusion, nor does the rule identify any reporting threshold for exceptions. Nevertheless, among other possible circumstances, companies are advised to consult with their counsel should one or more material weaknesses exist in their internal controls and procedures over financial reporting (which form a part of disclosure controls and procedures). In such circumstances, we believe it would be difficult to support any conclusion that the system of disclosure controls and procedures is effective.

Exchange Act rules existing prior to Sarbanes-Oxley require companies to maintain adequate internal accounting controls and provide reports that comply with SEC rules and regulations. Thus, public companies are already expected to maintain effective disclosure controls and procedures. Significantly, however, the new requirement to *explicitly* evaluate and report on that effectiveness raises issues about formalising the evaluation process.

## The Risks of an Informal Control Process

Under the oversight of their companies’ boards of directors, CEOs and CFOs should determine the level of formalisation for documenting and reviewing internal controls and procedures for financial reporting and disclosure controls and procedures. Having an appropriate degree of formalisation will enable them to make §302 certifications and provide §404 internal control reports with confidence, and will enable the appropriate level of review by third parties.

By now, it is expected that most public companies have met their initial reporting obligation concerning conclusions reached by their CEOs and CFOs about the effectiveness of their companies’ disclosure controls and procedures – or are at least well on their way to determining how they will satisfy that reporting obligation. Companies with relatively simple business environments and highly centralised management may be able to phase in new controls and procedures on an as-needed basis to support CEO and CFO certifications. Companies with more complex business activities, however, may conclude that such an approach is inadequate and subject to risk. But the bottom line is simple: All companies must assess how well their internal controls function and determine whether additional evaluation procedures are needed to ensure the soundness of CEO and CFO certifications.

The *ability of companies to demonstrate* that they have evaluated the effectiveness of their disclosure controls and procedures quarterly must not be overlooked. In addition, the SEC proposal, if adopted, will explicitly require quarterly evaluations of internal controls and procedures for financial reporting. As a result, every company *must be able to show* that it has an effective internal control system that provides reasonable assurance that all of its disclosures are complete, accurate, and timely, and that management has evaluated the critical control processes as required by Sarbanes-Oxley and related rules. CEOs, CFOs, and other management will be *well-served by documenting* the basis for such disclosures and conclusions – a process that will require documentation standards that go well beyond those of an informal review process.



Sarbanes-Oxley §408 requires the SEC to review disclosures made by each company reporting under the Exchange Act at least every three years. This means that a company should be prepared, when the SEC reviews its quarterly certifications and disclosures, to demonstrate the actions it has taken to ensure compliance and answer potential questions about whether any disclosures are missing or incomplete. In such cases, the SEC may ask about the underlying design, operation, and evaluation of a company's disclosure controls and procedures. If not satisfied, it may require amendments to previously disclosed information or impose other remedial actions that could result in unfavorable publicity or other negative consequences.

Another limitation of informal control processes is their tendency to be inefficient. This can lead to the need for substantial hands-on efforts to prepare certifications and other disclosures, especially by management at the end of each quarter. These efforts may include extensive testing and review to validate the completeness and accuracy of information. The connection between formalising the control process and increasing efficiency is further explored below under the sub-heading "The Benefit of Using an Internal Controls Maturity Framework."

## Operationalising the Control Process

Companies may find it helpful for the disclosure committee to focus on the design and effectiveness of disclosure controls and procedures as part of the committee's responsibility for determining required disclosures. This committee could function as a proactive agent within the organisation, encouraging robust analysis of the risks inherent in the company's activities and initiating discussions with senior officers to identify and address weaknesses in controls and procedures.

Companies that now have an informal internal control process may wish to integrate into their operations a more formal process for regularly monitoring and managing internal controls and procedures for financial reporting and disclosure controls and procedures, and reporting the results to executive officers. This process could be expected to include specific actions to be taken, under the direction of a disclosure committee, when preparing for a certification or other reporting on the effectiveness of a company's internal controls. Monitoring and managing activities might include:

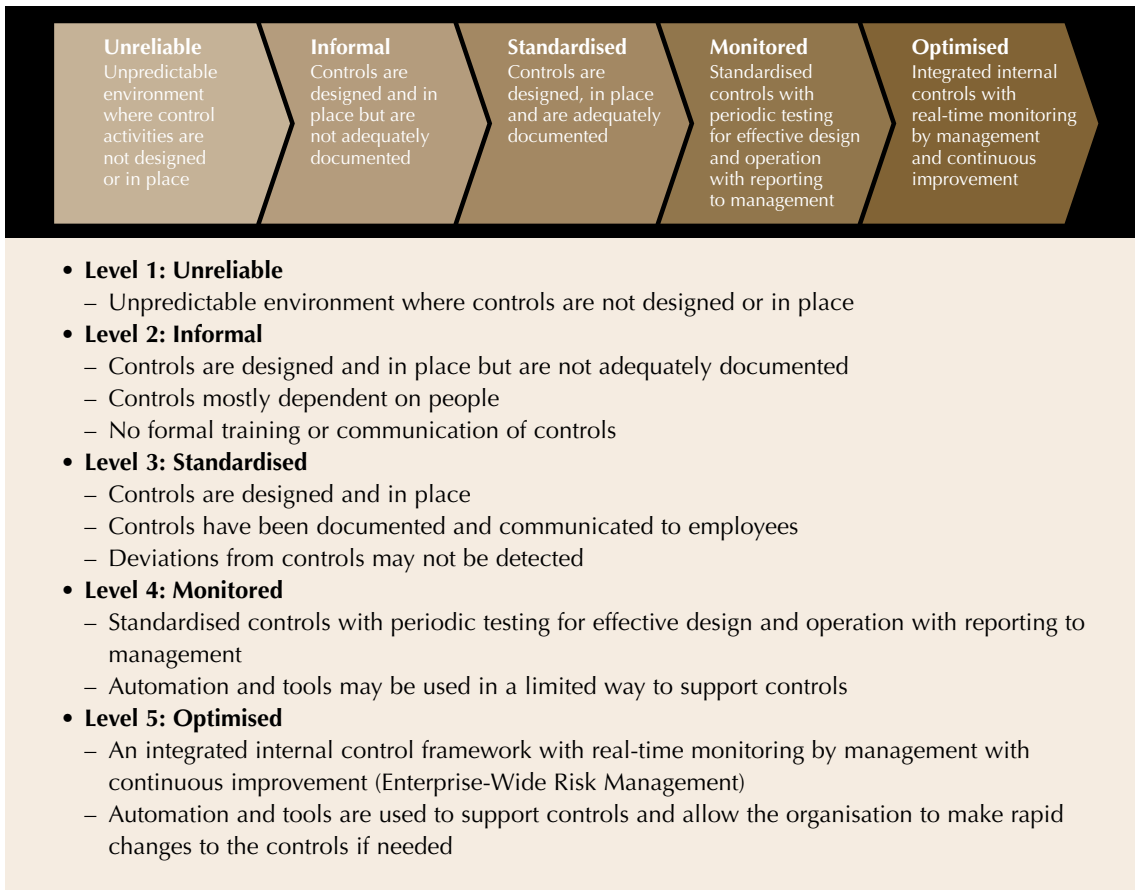
- Establishing reporting objectives
- Assigning and communicating responsibilities
- Assessing key risks and determining needed controls
- Providing employee training and implementing controls
- Monitoring and testing control effectiveness
- Remediating weaknesses that could adversely impact reporting obligations
- Reviewing results and proposed reporting

## The Benefit of Using an Internal Controls Maturity Framework

When evaluating a company's controls and procedures, companies may find it useful to apply an internal controls maturity framework. The primary objective of such a framework is to determine whether existing or proposed controls for a given activity or process are rigorous enough to manage related risks and sufficiently documented for subsequent internal and external review.

The following chart illustrates a hierarchy that we believe works well for categorising the maturity levels of controls.

## Internal Controls Maturity Framework



Use of such a maturity hierarchy could be helpful in evaluating internal controls and procedures for financial reporting and disclosure controls and procedures. Under the oversight of its board of directors, a company's management must ultimately determine the control level to use as a target for evaluating a company's internal controls. A primary consideration is that it is likely that a company's risk of penalties associated with missed, incomplete, or inaccurate disclosures is reduced the further it moves along the maturity framework. Other key factors to consider, beyond risk exposure, include a company's size and complexity, and the costs and benefits of formalising an internal control system.

Using an internal controls maturity framework provides a context to help CEOs and CFOs determine their comfort level with the controls that support certifications and other public reporting. This information enables them to decide whether the level of maturity for a given control area is satisfactory or whether remedial action needs to be taken.

In addition, an internal controls maturity framework can make it easier for a company to evaluate how its existing control structure impacts the level of effort required to meet its control reporting requirements. The following chart shows how increasing maturity levels for different control areas can improve efficiency, resulting in a process that works better and is less costly to maintain.

## Level of Efficiency May Be Influenced by Current Control Structure – A Hypothetical Illustration

### Current Control Structure

Effectiveness and Level of Documentation

#### High Efficiency

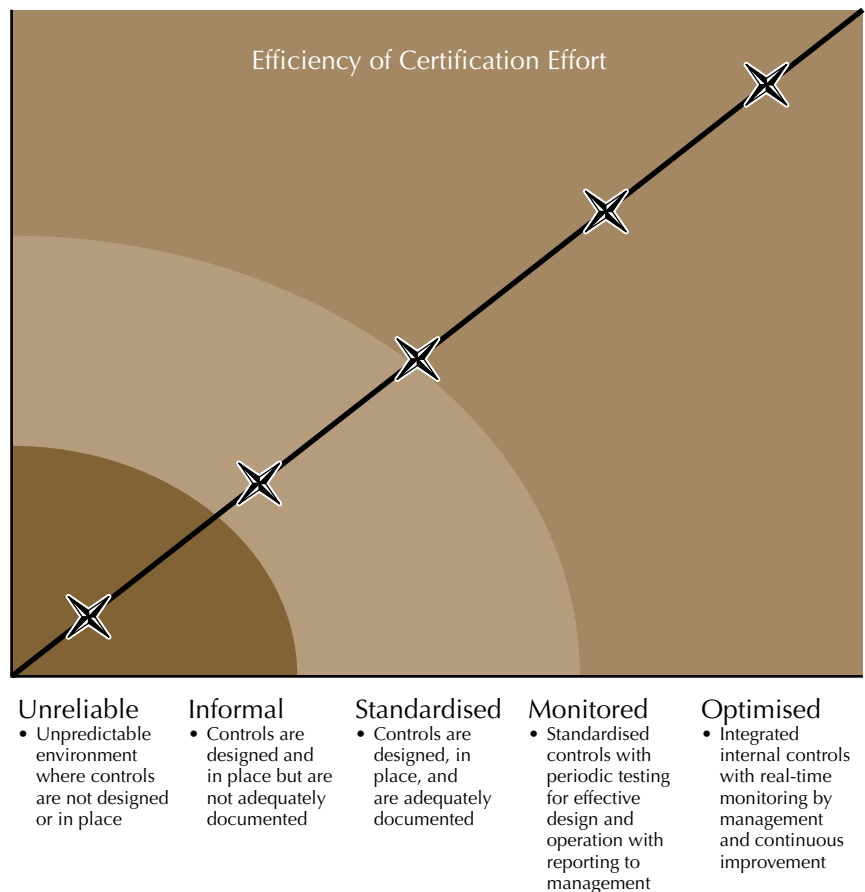
- Reliance on continual monitoring and review of periodic testing
- Use of dashboard for key indicators and controls
- Reliance on certifications and acknowledgements
- Management Time Commitment: Moderate

#### Medium Efficiency

- Some manual testing required for key activities
- Some reliance on monitoring
- Reliance on certifications and acknowledgements
- Management Time Commitment: Significant

#### Low Efficiency

- Substantial manual efforts
- Testing and validation required of activities
- Management Time Commitment: Substantial



## Developing an Action Plan and Beyond

As part of operationalising the control process, a disclosure committee may seek to develop an action plan for overseeing the performance of a quarterly review of its existing control structure and determining whether remedial actions are needed to satisfy relevant provisions of Sarbanes-Oxley and related rules. An effective action plan can help a company communicate what needs to be done, organise who will do it, and monitor and act on the results.

At the very least, a company's action plan should: (1) educate management and the board of directors, (2) mobilise those who will undertake the internal control effort, (3) collect information on the company's existing control structure, (4) assess the effectiveness of existing controls, and (5) perform remediation as needed and review proposed reporting.



Work performed during this review should be repeated or updated, as needed, to satisfy the SEC requirement for quarterly evaluations of the effectiveness of specified internal controls. Updates should focus on new required disclosures, the effectiveness of remediation efforts, and other changes that have occurred since the previous review.

The following are some examples of activities that can be helpful in tailoring an action plan to fit a company's needs:

### Educate Management and Board of Directors

1. Read Sarbanes-Oxley, the SEC rules, and other resources, such as this white paper.
2. Consult trusted advisers.
3. Attend seminars and workshops, especially those focused on Sarbanes-Oxley compliance issues for your industry.
4. Understand and communicate what is required and when.

### Mobilise

1. Establish a *disclosure committee*. This committee could be made responsible for establishing and supervising a company's entire disclosure process, becoming, in effect, the overseer for public disclosures. Such a committee would:
  - Have overall responsibility for developing communication and action plans and ensuring that the plans are carried out in a manner that will achieve the desired objectives.
  - Report to the CEO and CFO.
  - Include the controller, chief risk officer, and heads of compliance and/or legal, investor relations, operations, and individual business units.
2. Establish a *Sarbanes-Oxley project team* with defined roles and responsibilities. This team:
  - Should report to the disclosure committee.
  - Could include operations, finance, and compliance representatives for all business and operating units.
  - Should include dedicated project management resources.
3. Determine the approach, scope, timing, and resources needed to address certification and other disclosure requirements.





## Collect Information on Existing Control Structure

1. Inventory disclosures required in reports to the SEC and other stakeholders (required disclosures).
  - Consult with legal counsel as needed.
  - Review sources, such as SEC and other regulatory requirements, and disclosure checklists.
2. Review the company's recent regulatory reports and filings, and other disclosure communications, to identify current reporting disclosures and make note of any areas where additional disclosures may be required.
3. Inventory and document policies and procedures for accounting and reporting.
4. Inventory and document internal controls covering financial reporting, operations, and compliance.
  - Canvass all significant business and operating units to ensure adequate coverage.
  - Include flow charts, narratives, risk and control matrices, and other pertinent documentation.
5. Inventory and document known internal control issues and risks and existing remedial projects.
  - Review sources such as internal audit reports, external audit and regulatory reports, and employee complaints.
  - Consider industry and company-specific risks, focusing on sensitive areas.
6. Identify existing disclosure controls and supporting procedures. For each area requiring disclosure, identify and document the controls that management relies on to ensure that all material information related to a disclosure is (a) made known to them, (b) factually correct, and (c) available on a timely basis.
7. Develop and administer a risk culture survey within the company, if needed, to assess and document the control environment and "tone at the top" as described by COSO.

## Assess Effectiveness of Controls

1. Target: Determine the targeted maturity level of controls supporting various areas of financial reporting and other required disclosures.
  - Refer to the internal controls maturity framework to establish criteria for maturity levels.
  - Establish a targeted maturity level based on the various factors that impact the effectiveness and efficiency of supporting controls.
2. Existing condition: Review existing controls supporting each area of financial reporting and other required disclosures.
  - Assess the design of existing controls using the COSO framework.
  - Test whether existing controls are functioning as designed, to the extent not already tested.
  - Use the internal controls maturity framework to determine the maturity level of existing controls.
  - Consider the above results and any other relevant factors, using COSO criteria, in determining the effectiveness of existing controls.
3. Gap analysis: Based on the above assessment, identify and document areas of financial reporting and other required disclosures for which:
  - The maturity level of existing controls is lower than the targeted level.
  - The existing controls are not deemed to be effective.

## Perform Remediation and Review Proposed Reporting

1. Use gap analysis to identify and prioritise necessary projects.
  - Identify and initiate remedial projects that are necessary to move toward the targeted control maturity level and enable existing controls to adequately support the certification and other reporting requirements. Consider the timeline for these projects relative to intervening reporting periods, taking into account the system of internal controls viewed as a whole.
  - Undertake substantive procedures to support any financial reporting or other required disclosures for which existing controls cannot be readily remediated to an acceptable level.
  - Consider longer-term goals for the control process, such as enhancing effectiveness and efficiency, as a basis for identifying and prioritising improvement projects.
2. Perform other control-related activities before submitting the report for the current period to the SEC.
  - Consider getting assurances from key personnel about completion of assignments and whether they are aware of any additional disclosures that may be required or of significant deficiencies in existing controls.
  - Disclose to the audit committee and external auditor, in writing, any significant deficiencies and material weaknesses identified in internal controls and procedures for financial reporting and any remedial actions taken, as well as any fraud involving a person who plays a significant role in the internal control process.
  - Review all representations to be provided in the CEO and CFO certification and other financial and non-financial disclosures to be provided in the current periodic report to the SEC.

## Aligning Reporting Obligations with Strategic Management

### Strategic Management Needs

When designing control structures, top executives are looking beyond the basic objective of implementing effective internal controls to satisfy financial and other reporting obligations. They recognise that to be a leader in serving customers in today's demanding business environment, a company must have a dynamic risk management process that covers critical risk exposures and enables the company to identify and respond quickly to changing conditions.

To make such a risk management process highly effective, it should be built into a company's infrastructure as an integral part of doing business and tailored to the company's critical risk exposures. This integrated approach to managing risk and change across the organisation is commonly referred to as "enterprise-wide risk management." A primary objective is to enable the company to identify, assess, monitor, and manage changes of all types that may impact its risk exposures and opportunities. A company with that capability is better able to proactively manage many different risk exposures and seize business opportunities that can potentially create a competitive advantage.



An enterprise-wide risk management structure should incorporate a number of key elements, such as:

- An integrated, dynamic display of business objectives, key risks, and controls that are aligned with supporting policies, procedures, and operating principles.
- A robust, flexible structure that can deal systematically with both external and internal changes affecting the company.
- Monitoring of key risk exposures on a real-time basis and exception reporting to management.
- An aligned and supportive infrastructure that facilitates early identification of new business risks, communication, training, incident identification, issues management, and internal and external reporting.

## Linking Enterprise-Wide Risk Management with Sarbanes-Oxley

If a company chooses to use enterprise-wide risk management, a critical risk exposure that should be covered is compliance with laws and regulations, including Sarbanes-Oxley and related rules. An enterprise-wide risk management structure can provide a strong platform and dynamic, integrated tools for managing that exposure.

Exposure management would include having effective, validated controls supporting financial and other reporting obligations that are linked to the company's business, operations, and compliance requirements. Such controls should cover all components identified in COSO or a similar framework, and should embrace designing, maintaining, evaluating, and reporting on effective control systems as required by Sarbanes-Oxley and other laws and regulations.

As part of an enterprise-wide risk management structure, the control process should include real-time monitoring of control testing and effectiveness for all areas. This monitoring should cover key controls supporting required disclosures to executive management, directors, and the public. It should flag changes affecting those disclosures to enable management to continuously fine-tune monitoring efforts and take other appropriate actions. For example, real-time monitoring should alert management about key developments related to the company's business to enable prompt public disclosure as may be required by Sarbanes-Oxley §409.

The risk management structure should also provide key indicators confirming the effectiveness of controls and procedures supporting financial reporting and other required disclosures, and generate much of the information needed to prepare quarterly CEO and CFO certifications and other reports.

Having integrated internal controls that include real-time monitoring by management and continuous improvement in response to changing conditions provides an "optimised" maturity level for controls, as defined in the internal controls maturity framework described earlier. Achieving this maturity level should provide high assurance of control effectiveness and can lower an organisation's incremental costs for complying with new laws such as Sarbanes-Oxley. It can also help achieve greater transparency in corporate reporting by enabling management to provide timely and reliable disclosures to all stakeholders.



## IV. Conclusion: A New Beginning

Sarbanes-Oxley marks the beginning of a new reporting era for public companies. Many of its requirements are broad and untested, but expectations by both the public and regulators are high. In the early reporting stages, some companies will of necessity respond with “fire-drill” or add-on reviews of controls in order to fulfill their reporting responsibilities. Over the long term, however, companies will need to build in the required processes to ensure that their corporate reporting on internal controls is part of the way they do business, not just an afterthought.

No company can afford to ignore the new reporting requirements, even though SEC rules impacting a number of key areas have yet to be finalised. CEOs and CFOs must be committed and prepared to comply with all rules as they become effective to avoid the risk of the tough civil and criminal penalties that are built into Sarbanes-Oxley. In particular, they must understand Sarbanes-Oxley and SEC reporting obligations and guide their companies in managing compliance efforts. By having effective control structures in place to meet these obligations, including the required review and evaluation procedures, companies can provide complete, accurate, and trustworthy information to their stakeholders.

The strategies and actions presented in this paper are intended to assist company leaders in developing and executing effective, pragmatic, and tailored plans in meeting the Sarbanes-Oxley challenge.

Companies that succeed in these efforts will be able to satisfy reporting requirements to shareholders, the public, directors, and other stakeholders with greater confidence. They will also benefit from the enhanced credibility that comes from quality corporate reporting – a key advantage that can have a positive impact on both their cost of capital and their ability to operate at peak effectiveness.

## Appendix A: Summary of the Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act of 2002 establishes new standards for corporate accountability as well as penalties for corporate wrongdoing. The legislation contains 11 titles, ranging from additional responsibilities for audit committees to tougher criminal penalties for white-collar crimes such as securities fraud. The SEC is required to issue rules implementing several of these provisions. The rules eventually issued by the SEC may go beyond the statutory requirements.

Here is a summary of each of the 11 titles:

### Title I – Public Company Accounting Oversight Board

- Establishes an independent, non-governmental board to oversee the audits of public companies to protect the interests of investors and further public confidence in independent audit reports.
- Defines the major responsibilities of this board.
- Requires public accounting firms to register with the board and take certain other actions in order to perform audits of public companies.

### Title II – Auditor Independence

- Sets forth required actions by registered public accounting firms (“external auditors”), audit committees and companies that are intended to strengthen auditor independence.
- Legislates certain services, generally consistent with current independence rules, as unlawful if performed by the external auditor.

### Title III – Corporate Responsibility

- Requires audit committees to be independent and undertake specified oversight responsibilities.
- Requires CEOs and CFOs to certify quarterly and annual reports to the SEC, including making representations about the effectiveness of specified controls.
- Provides rules of conduct for companies and their officers regarding pension blackout periods and certain other matters.
- Requires the SEC to issue rules requiring attorneys in certain roles to report violations of securities laws to a company’s CEO or chief legal counsel and, if no action is taken, to the audit committee.

### Title IV – Enhanced Financial Disclosures

- Requires companies to provide enhanced disclosures, including a report on the effectiveness of internal controls and procedures for financial reporting (along with external auditor attestation of that report) and disclosures covering off-balance sheet transactions and pro forma financial information.
- Requires disclosures regarding code of ethics for senior financial officers and reporting of certain waivers.
- Requires accelerated disclosures by management, directors, and principal stockholders concerning certain transactions involving company securities.

### Title V – Analyst Conflicts of Interest

- Requires the SEC to adopt rules to address conflicts of interest that can arise when securities analysts recommend equity securities in research reports and public appearances.

### Title VI – Commission Resources and Authority

- Provides additional funding to the SEC.
- Gives the SEC and federal courts more authority to censure and impose certain prohibitions on persons and entities.

### Title VII – Studies and Reports

- Directs federal regulatory bodies to conduct studies regarding consolidation of accounting firms; credit rating agencies; violators, violations, and enforcement actions involving securities laws; certain roles of investment banks and financial advisors; and certain other matters.

### Title VIII – Corporate and Criminal Fraud Accountability

- Provides tougher criminal penalties for altering documents, defrauding shareholders, and certain other forms of obstruction of justice and securities fraud.
- Makes debts non-dischargeable if incurred in violation of securities fraud laws.
- Protects employees of companies who provide evidence of fraud.

### Title IX – White-Collar Crime Penalty Enhancements

- Provides that any person who attempts to commit white-collar crimes shall be treated under the law as if the person had committed the crime.
- Enhances penalties and sentencing guidelines for certain white-collar crimes such as mail and wire fraud and ERISA violations.
- Requires CEOs and CFOs to certify in their periodic reports to the SEC that their financial statements fully comply with the requirements of the Securities Exchange Act of 1934, and imposes penalties for certifying a misleading or fraudulent report.

### Title X – Corporate Tax Returns

- Conveys the sense of the Senate that the CEO should sign a company's federal income tax return.

### Title XI – Corporate Fraud and Accountability

- Provides additional authority to regulatory bodies and courts to take various actions, including fines or imprisonment, with regard to tampering with records, impeding official proceedings, taking extraordinary payments, retaliating against corporate whistleblowers, and certain other matters involving corporate fraud.

## Appendix B: Effective Dates of Principal Provisions in Sarbanes-Oxley Titles III and IV

The following effective dates have been identified for principal provisions contained in Titles III and IV of Sarbanes-Oxley and related SEC rules directly affecting public companies.

By July 30, 2002:

- Forfeiture by CEO and CFO of bonuses and profits from security sales in the event of a restatement of financial statements (§304)
- Prohibition of certain loans to directors and executive officers (§402)

By August 29, 2002:

- Required CEO and CFO certifications of quarterly and annual reports (§302 and SEC rule)
- Reporting by executives, directors, and principal stockholders within two business days of certain transactions involving company securities (§403 and SEC rule)

By October 28, 2002:

- Deadline for SEC to propose rules covering:<sup>24</sup>
  - Improper influence on the conduct of an audit (§303)
  - Code of ethics for senior financial officers (§406)
  - Audit committee “financial expert” (§407)

By January 26, 2003:

- SEC to issue final rules covering several matters such as:<sup>25</sup>
  - Pension fund blackout periods (§306)
  - Disclosure of material off-balance sheet transactions and arrangements (§401)
  - Presentation of pro forma financial information (§401)
  - Code of ethics for senior financial officers (§406)
  - Audit committee “financial expert” (§407)



By April 26, 2003:

- SEC to issue final rules:
  - Directing securities exchanges to prohibit a company not complying with the amended audit committee rules from listing any security (§301)
  - Improper influence on the conduct of an audit (§303)<sup>26</sup>

By January 26, 2004:

- SEC to complete study of extent of off-balance sheet transactions, including use of special purpose entities, and the transparency of the treatment of those transactions under generally accepted accounting principles (§401)

No Deadline Specified in Sarbanes-Oxley:

- Required internal control reports by companies (§404)<sup>27</sup>
- Required “real-time” disclosure of information concerning material changes in the company’s financial condition or operations (§409)



## Notes

- 1 U.S. Congress, *Sarbanes-Oxley Act of 2002*, Pub. L. 107-204, 116 Stat. 745 (2002). This legislation can be accessed at: [http://financialservices.house.gov/media/pdf/H3763CR\\_HSE.PDF](http://financialservices.house.gov/media/pdf/H3763CR_HSE.PDF).
- 2 Samuel A. DiPiazza, Jr. and Robert G. Eccles for PricewaterhouseCoopers, *Building Public Trust – The Future of Corporate Reporting* (New York: John Wiley & Sons, Inc., 2002).
- 3 As used in this paper, “public companies” or “companies” refers to those companies covered by Sarbanes-Oxley; in general:
  - Companies that have a class of securities registered under Section 12 or are required to file reports under Section 15(d) of the Exchange Act of 1934 (including foreign private issuers, banks and savings associations, issuers of asset backed securities, and small business issuers that have a reporting obligation under those sections of the Exchange Act).
  - Companies filing registration statements that have not yet become effective under the Securities Act of 1933 and that have not been withdrawn.
- 4 *Building Public Trust*, pages 3–6.
- 5 U.S. Securities and Exchange Commission, “Final Rule: Certification of Disclosure in Companies’ Quarterly and Annual Reports,” 17 CFR Parts 228, 229, 232, 240, 249, 270 and 274; Release Nos. 33-8124, 34-46427, IC-25722; File No. S7-21-02, RIN 3235-AI54 (Washington, D.C.: U.S. Securities and Exchange Commission, August 29, 2002).
- 6 The SEC certification rule also requires registered investment companies that file periodic reports under Section 13(a) or 15(d) of the Exchange Act to include CEO and CFO certifications in those reports.
- 7 The SEC has proposed a modification that, if adopted, would require making the evaluation as of the end of the period covered by the report. This change is proposed to apply initially to a company’s certification in its annual report to the SEC for a fiscal year ending on or after September 15, 2003. See U.S. Securities and Exchange Commission, “Proposed Rule: Disclosure Required by Sections 404, 406 and 407 of the Sarbanes-Oxley Act of 2002,” 17 CFR Parts 210, 228, 229, 240, 249, 270 and 274; Release Nos. 33-8138, 34-46701, IC-25775; File No. S7-40-02, RIN 3235-AI66 (Washington, D.C.: U.S. Securities and Exchange Commission, October 22, 2002).
- 8 Ibid. This change is proposed to apply initially to a company’s certification in its annual report for a fiscal year ending on or after September 15, 2003.
- 9 Ibid.
- 10 Other than by a registered investment company, which has special rules.
- 11 American Institute of Certified Public Accountants, Professional Standards – Attestation Standards, AT §501, “Reporting on an Entity’s Internal Controls over Financial Reporting.”
- 12 Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control – Integrated Framework* (New York: American Institute of Certified Public Accountants, 1992). This report, which can be obtained from the AICPA, is in four volumes:
  - Volume 1, “Executive Summary,” is a high-level overview of the internal control framework directed to the chief executive and other senior executives, board members, legislators, and regulators.
  - Volume 2, “Framework,” defines internal control, describes its components, and provides criteria against which managements, boards, or others can assess their control systems.
  - Volume 3, “Reporting to External Parties,” is a supplemental document providing guidance to those entities that report publicly on internal control over preparation of their published financial statements.
  - Volume 4, “Evaluation Tools,” provides materials that may be useful in conducting an evaluation of an internal control system.

- 13 American Institute of Certified Public Accountants, Codification of Statements on Auditing Standards AU §319, "Consideration of Internal Control in a Financial Statement Audit."
- 14 *Internal Control – Integrated Framework, Volume 1*, "Executive Summary."
- 15 *Internal Control – Integrated Framework, Volume 2*, "Framework," page 9.
- 16 AU §319.
- 17 *Internal Control – Integrated Framework, Volume 1*, "Executive Summary."
- 18 *Internal Control – Integrated Framework, Volume 2*, "Framework," pages 14–15.
- 19 Ibid.
- 20 "Proposed Rule: Disclosure Required by Sections 404, 406 and 407 of the Sarbanes-Oxley Act of 2002."
- 21 AU §325.
- 22 American Institute of Certified Public Accountants, Professional Standards – Attestation Standards, AT §101, "Attest Engagements," Sections 101.23–101.32.
- 23 "Final Rule: Certification of Disclosure in Companies' Quarterly and Annual Reports."
- 24 The SEC has proposed rules covering these Sarbanes-Oxley provisions.
- 25 Ibid.
- 26 Ibid.
- 27 "Proposed Rule: Disclosure Required by Sections 404, 406 and 407 of the Sarbanes-Oxley Act of 2002."



PricewaterhouseCoopers ([www.pwc.com](http://www.pwc.com)) is the world's largest professional services organisation. Drawing on the knowledge and skills of more than 125,000 people in 142 countries, we build relationships by providing services based on quality and integrity.

Your worlds



Our people

[www.pwc.com](http://www.pwc.com)

© 2002 PricewaterhouseCoopers. All rights reserved. PricewaterhouseCoopers refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity.